Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] A method for facilitating biometric security in a smart-card transaction system, said method comprising:
determining if a transaction violates an established rule;
notifying a user to proffer a biometric sample to verify the identity of said user;
detecting a proffered biometric at a sensor communicating with said system to obtain a proffered biometric sample;
verifying the proffered biometric sample; and
authorizing said transaction that violates an established rule to proceed upon verification of the proffered biometric sample.

[c2] The method of claim 1, wherein said step of determining if a transaction violates an established rule includes determining if said transaction is at least one of a purchase exceeding an established per purchase spending limit, a purchase exceeding a preset number of transactions, any portion of a purchase using non-monetary funds, and a purchase exceeding an established limit.

[c3] The method of claim 1, wherein said step of notifying includes providing notification by at least one of an audi-

ble signal, visual signal, optical signal, mechanical signal, vibration, blinking, signaling, beeping, providing an olfactory signal, providing a physical touch signal, and providing a temperature signal to said user.

[c4] The method of claim 1, wherein said step of detecting further includes detecting a proffered biometric at a sensor configured to communicate with said system via at least one of a smartcard, reader, and network.

[c5] The method of claim 1, wherein said step of detecting includes at least one of: detecting, storing, and processing a proffered biometric sample.

[c6] The method of claim 1, wherein said step of detecting includes receiving a finite number of proffered biometric samples during a transaction.

[c7] The method of claim 1, wherein said step of detecting includes logging each proffered biometric sample.

[c8] The method of claim 1, wherein said step of detecting includes at least one of detecting, processing and storing at least one second proffered biometric sample.

[c9] The method of claim 1, wherein said step of verifying includes comparing a proffered biometric sample with a stored biometric sample.

[c10] The method of claim 9, wherein comparing a proffered biometric sample with a stored biometric sample includes comparing a proffered biometric sample with a biometric sample of at least one of a criminal, a terrorist, and a cardmember.

[c11] The method of claim 1, wherein said step of verifying includes verifying a proffered biometric sample using information contained on at least one of a local database, a remote database, and a third-party controlled database.

[c12] The method of claim 1, wherein said step of verifying includes verifying a proffered biometric sample using one of a local CPU and a third-party security vendor.